Учебный центр компьютерного обучения «СПЕЦИАЛИСТ» при МГТУ им. Н.Э.Баумана

«VPN для пользователя»

Захаров Николай Михайлович

Захаров Николай Михайлович

Заведующий лабораторией вычислительных машин МГТУ им. Н.Э. Баумана
Ведущий преподаватель ЦКО «Специалист» при МГТУ им. Н.Э. Баумана по направлению «Настройка и ремонт ПК, HelpDesk»

- **MCP – Microsoft Certified Professional**
- **Apple Certified Support Professional**
- **CompTIA Certified Service Professional**
- **Paragon Certified Trainer**
- **Тренер Dr.Web (по комплексной антивирусной и антиспам защите Windows-систем)**

VPN (Virtual Private Network) — виртуальная частная сеть.

С повсеместным распространением высокоскоростного Интернета проблема приватности в сети встала особенно остро.
Людям стало важно не только иметь возможность подключаться к Интернету в любом месте, но и чувствовать себя защищенными от подслушивания, перехвата личных данных, да и просто чувствовать себя на просторах всемирной сети более уверенно.
Попробуем разобраться, что же такое VPN и как нам может пригодиться эта технология.

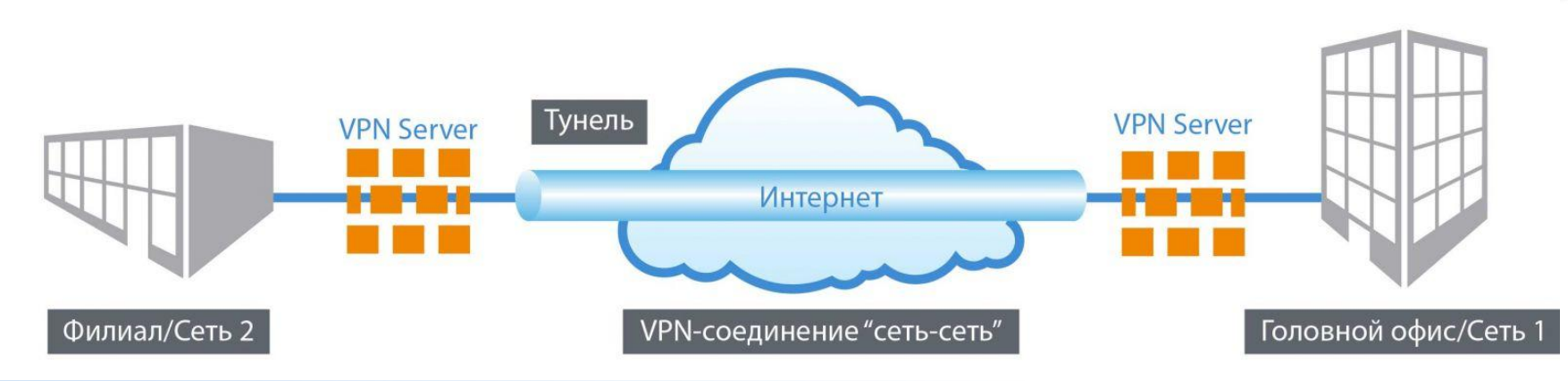
Что такое VPN?

Зачем нужен VPN-сервис?

Некоторые, наиболее типичные сценарии использования VPN.

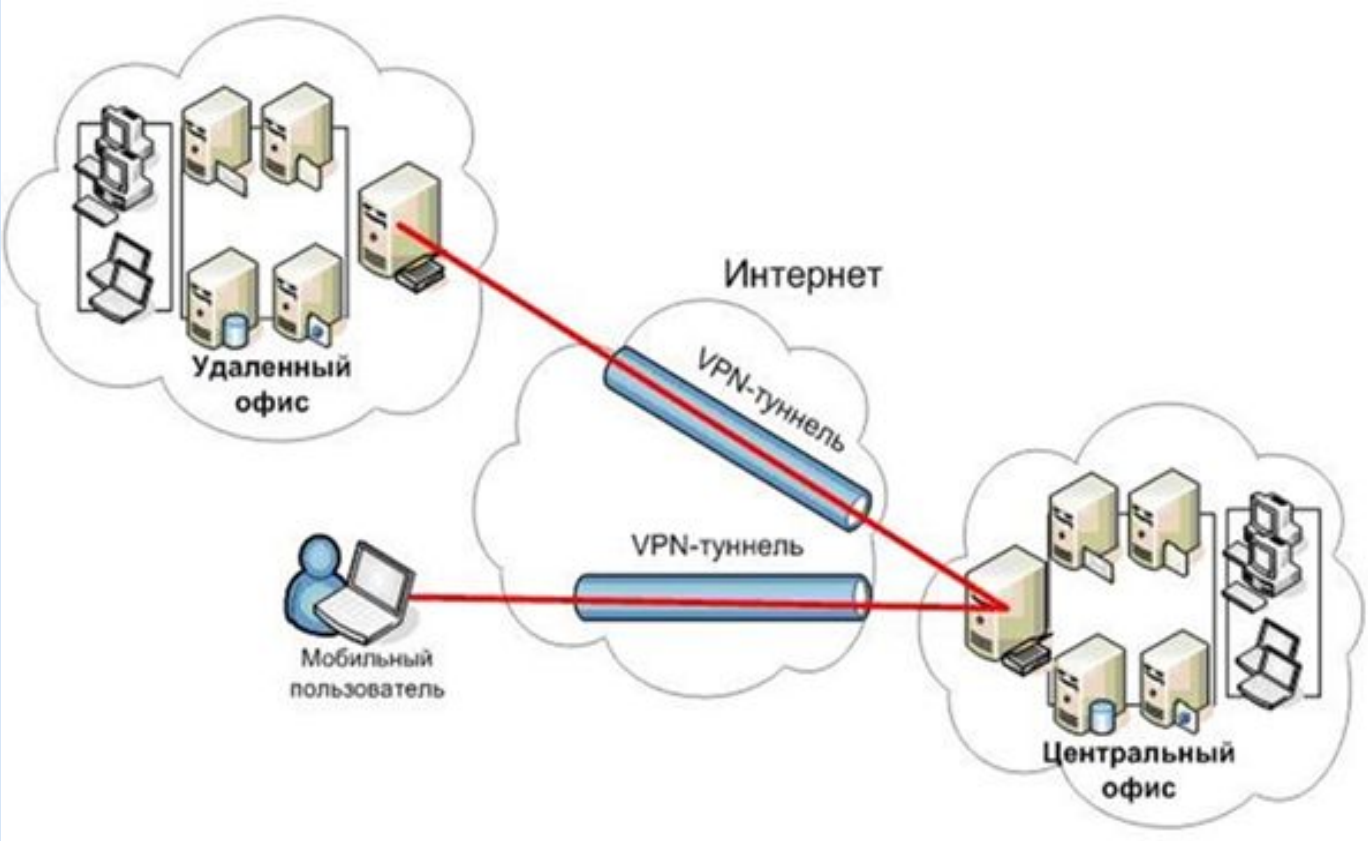
Корпоративные сети

1. Использование VPN для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.



Корпоративные сети

2. Использование VPN для создания защищённого канала (туннеля), между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая вне офиса, подключается к корпоративным ресурсам с удаленного компьютера.



Между пользователем и сетевым ресурсом создается виртуальный канал связи.

Всё выглядит так, как будто к удаленному компьютеру пользователя подключили сетевой кабель протянутый прямиком из офиса.
Все офисные ресурсы (принтеры компьютеры коллег, файл-серверы) становятся доступными.
А на самом деле весь сетевой трафик шифруется, передаётся через общедоступную сеть (Internet) на VPN-сервер в офисе так, что злоумышленники не могут перехватить его реальное содержимое.
Т.е. физически вы находитесь в сети какого-то интернет-провайдера, но виртуально как будто бы сидите в офисе на работе.

Применение VPN в частном порядке

У обычного пользователя есть 3 основные причины для работы в сети через VPN.

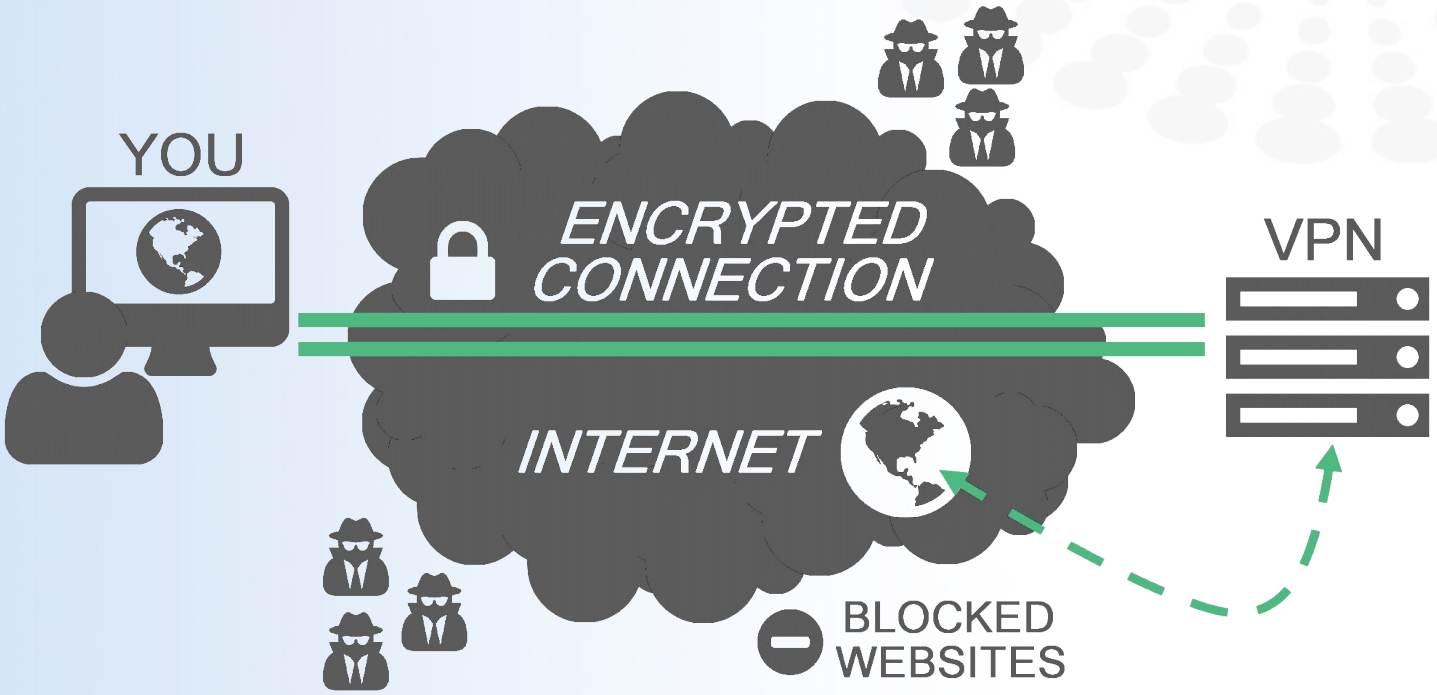
1. Защита данных, передаваемых по сети.
Без защиты ваши личные данные, в том числе банковские данные и номера кредитных карт, могут попасть в чужие руки! Хороший VPN зашифрует все ваши данные, так что даже при подключении к публичной точке доступа Wi-Fi вся ваша конфиденциальная информация будет под защитой.

Применение VPN в частном порядке

2. Гео-блокировки.

По инициативе правительства или команды того или иного сервиса доступ к некоторым сайтам может быть заблокировать для жителей соответствующего региона.

С помощью VPN трафик будет перенаправлен на другой сервер, расположенный в другом регионе или стране, что позволит обойти блокировки доступа



Применение VPN в частном порядке

3. Анонимность работы в сети Интернет.

Сервисы VPN обеспечивают простой и надежный способ для анонимного и конфиденциального просмотра с изменением IP адреса

Даже провайдер не будет знать, какие ресурсы посещает пользователь, а ресурсы не поймут, кто их посетил.

Для реализации VPN необходимо настроить VPN-сервер, а подключение к нему происходит с помощью VPN-клиента, настроенного на пользовательском устройстве.

В роли VPN-сервера могут выступать: сервера Unix, сервера Windows или сетевые маршрутизаторы.
Сейчас встроенные VPN-клиенты есть во всех актуальных операционных системах, в том числе в Windows, macOS, Linux, Android, iOS.

Для создания VPN сети (VPN канала) на сервере и клиенте используется специальное программное обеспечение, которое работает над драйверами сетевых карт - протоколы для построения VPN-туннеля

PPTP (Point-to-Point Tunneling Protocol)

Поддерживается буквально всеми ОС, даже очень старыми.
По умолчанию шифрование не используется.

Плюсы

- Высокая скорость
- Встроенный клиент практически на всех платформах.
- Простая настройка

Минусы

- Протокол взломан Агентством национальной безопасности США
- Не гарантирует полную безопасность

L2TP и L2TP/IPsec

L2TP (Layer 2 Tunneling Protocol) - протокол туннелирования уровня 2 (канального уровня)

IPSec (Internet Protocol Security) — это целый набор протоколов, стандартов и рекомендаций, специально разработанный для создания безопасных соединений в Сети.

L2TP считается более эффективным для построения виртуальных сетей, хотя и чуточку более требователен к вычислительным ресурсам по сравнению с PPTP.

L2TP по умолчанию также не предлагает шифрования и используется одновременно с другими протоколами — как правило, это IPSec.

Плюсы

- Считаются относительно безопасными протоколами
- Доступны в большинстве систем и почти на всех устройствах
- Простая настройка

Минусы

- Защита протокола нарушена Агентством национальной безопасности США
- Сложно использовать при наличии блокировки со стороны брандмауэра

SSTP (Secure Socket Tunneling Protocol)

Впервые этот протокол был представлен компанией Microsoft в SP1 для Windows Vista, на сегодня этот протокол доступен для Linux, RouterOS, но преимущественно он рассчитан для работы в Windows.

Плюсы

- Позволяет обходить большинство файрволов
- Уровень безопасности зависит от выбранного шифра, обычно он достаточно высокий.
- Хорошее взаимодействие с ОС Windows
- Поддержка Microsoft

Минусы

- Работает только на платформе Windows

IKEv2 (Internet Key Exchange Protocol)

Это протокол туннелирования (протокол обмена ключами, версия 2), разработанный Cisco и Microsoft, он встроен в Windows 7 и последующие версии.

Плюсы

- Высокая степень безопасности — поддержка различных шифров, в частности 3DES, AES, AES 256.
- Стабильно подключается снова после разрыва соединения или смены сетей
- Просто установить и настроить, по крайней мере, для пользователя
- Быстрее, чем L2TP, PPTP и SSTP

Минусы

- Поддерживает малое количество платформ.
- Исходный код не открыт

OpenVPN

Относительно новая технология с открытым исходным кодом. Обеспечивает надежное и мощное VPN-решение для пользователей.

Протокол OpenVPN является самым безопасным на данный момент.

Плюсы

- Позволяет обходить большинство файрволов
- Гибкая настройка
- Открытый исходный код — может быстро адаптироваться к новым опасностям
- Совместим с различными алгоритмами шифрования
- Высокая степень безопасности

Минусы

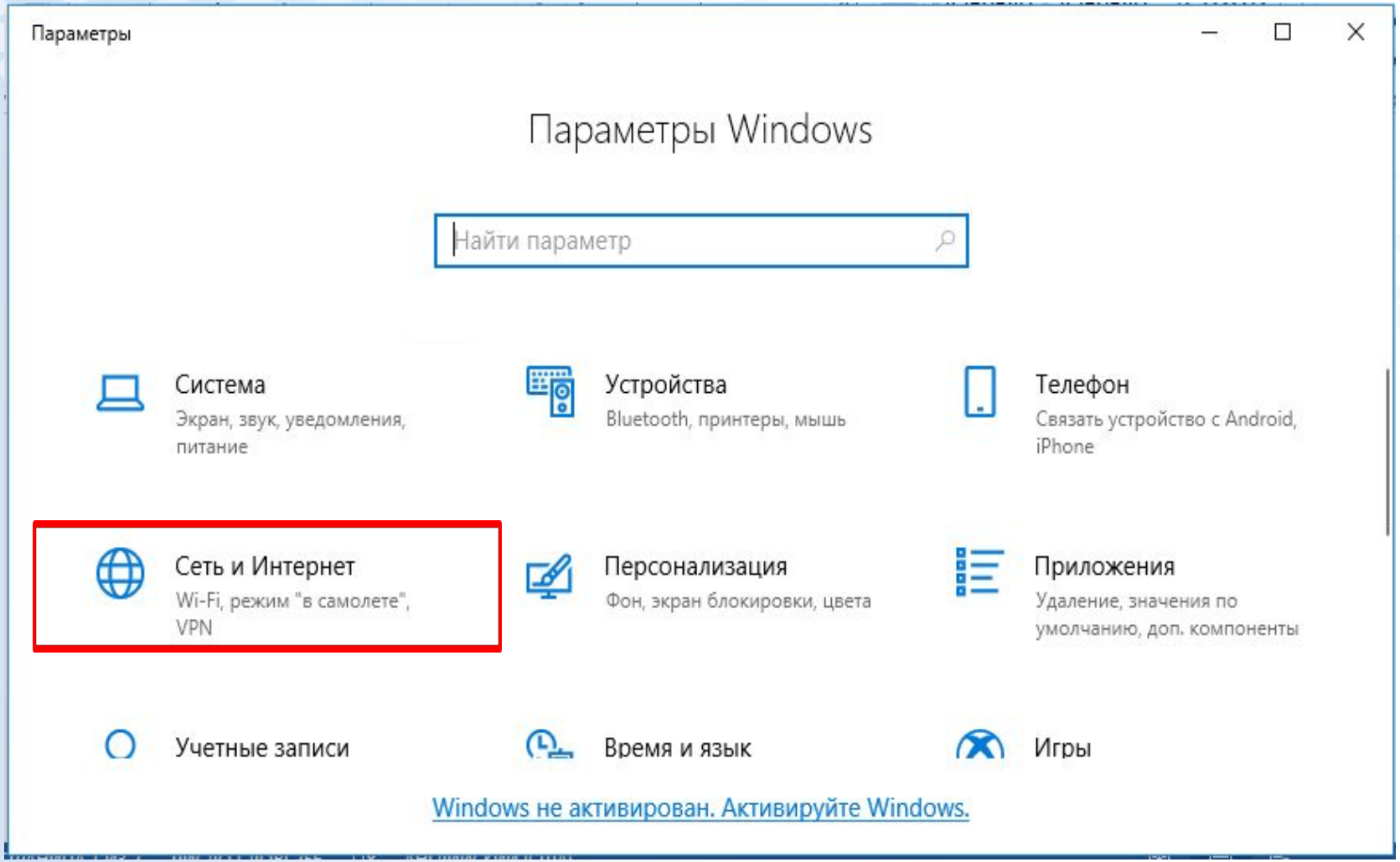
- Поддержка компьютеров неплоха, но на мобильных устройствах протокол работает не лучшим образом.

Подбор VPN сервиса

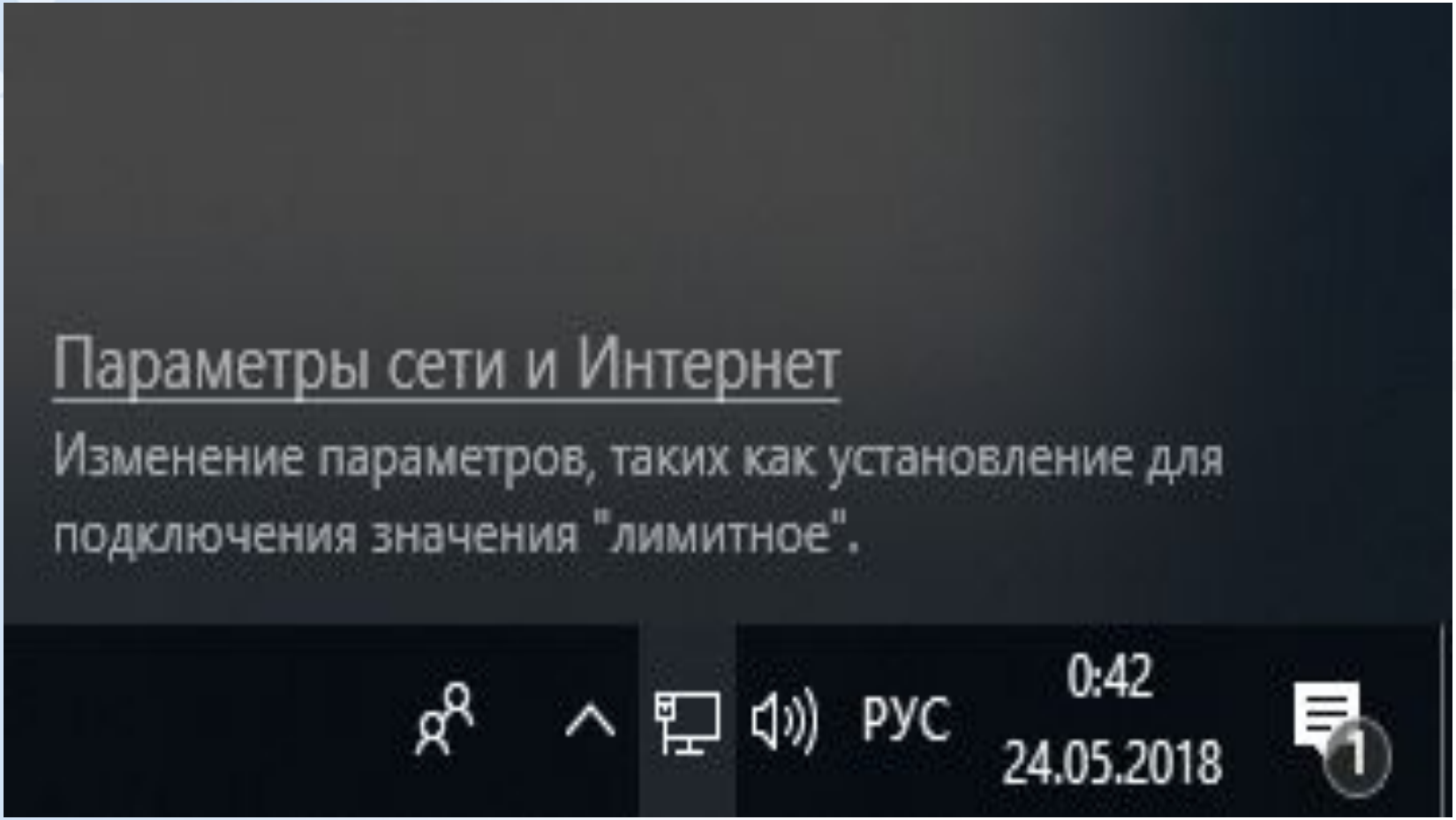
В Интернет существует множество сайтов VPN-провайдеров, которые предлагают различные VPN-сервисы, платные и бесплатные.
Существуют сайты, которые составляют рейтинги VPN сервисов, определяют наиболее качественные на их взгляд и предлагают их к использованию.
ru.vpnmentor.com/
www.vpnlist.ru
Бесплатные онлайн ресурсы, предоставляющие VPN доступ, зачастую грешат обилием показываемой рекламы. Также этот класс сервисов отличается не самыми современными методами шифрования, которые снижают степень защищенности информации. Соединение с интернетом через бесплатный VPN обычно замедляется.
Платные VPN сервера отличаются лучшей стабильностью и предоставляют доступ в сеть на большей скорости, чем большинство бесплатных.

Настройка VPN клиента в Windows 10

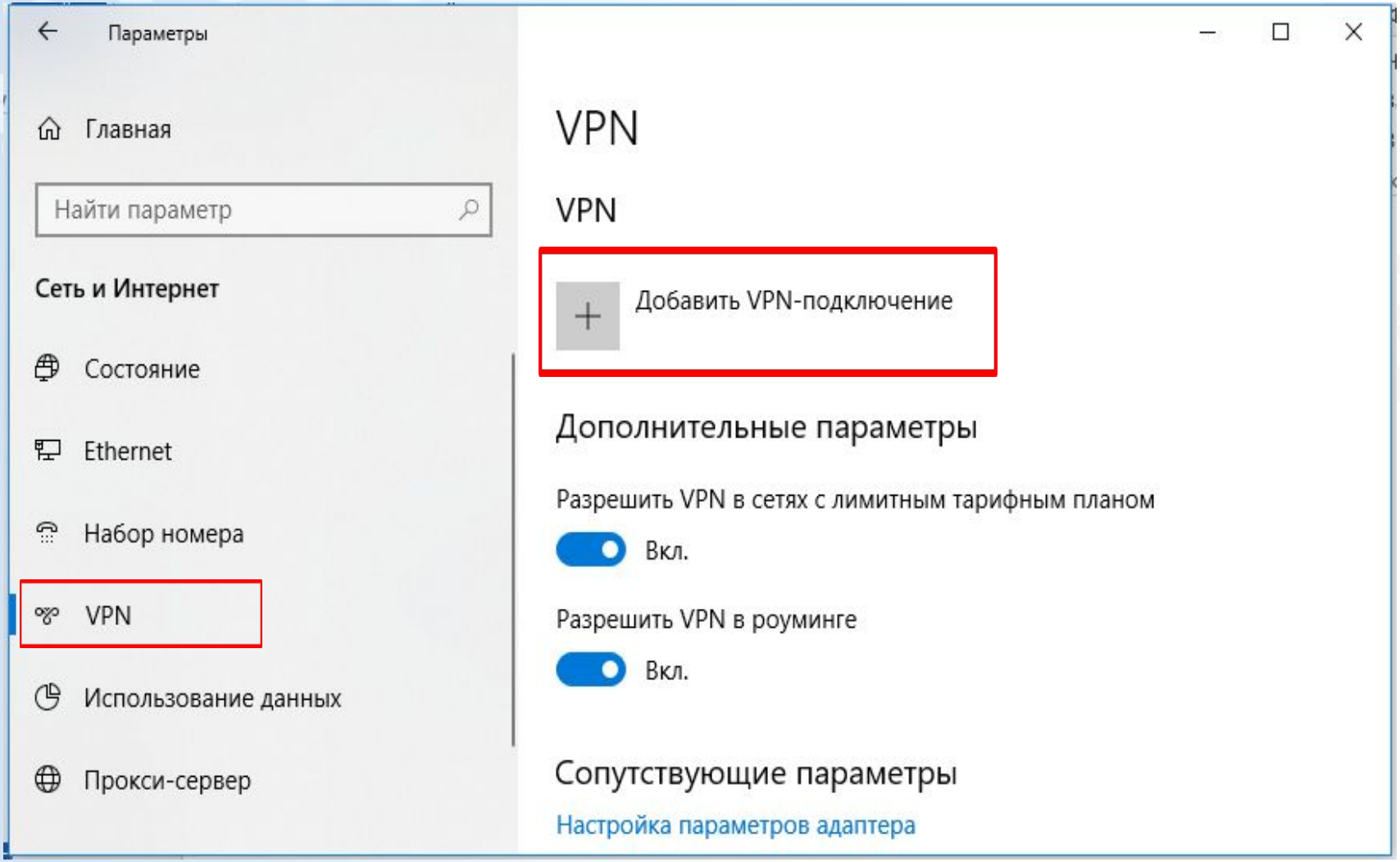
1. Параметры Windows - Сеть и Интернет



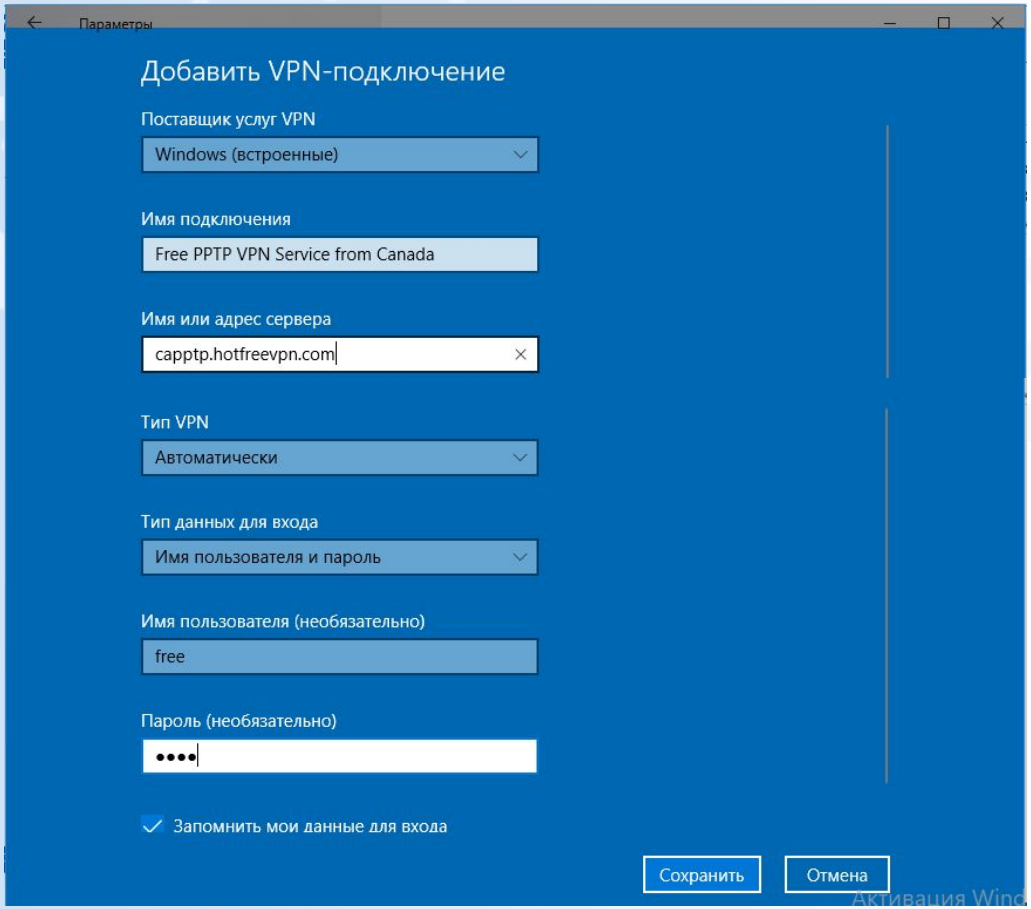
2. Кликнуть на иконке сетевого подключения в системном трее, и в появившемся окне выбрать Параметры сети и Интернет.



В окне Сеть и Интернет выбрать VPN и кликнуть на Добавление VPN-подключения.



В открывшемся окне заполнить данные для подключения:



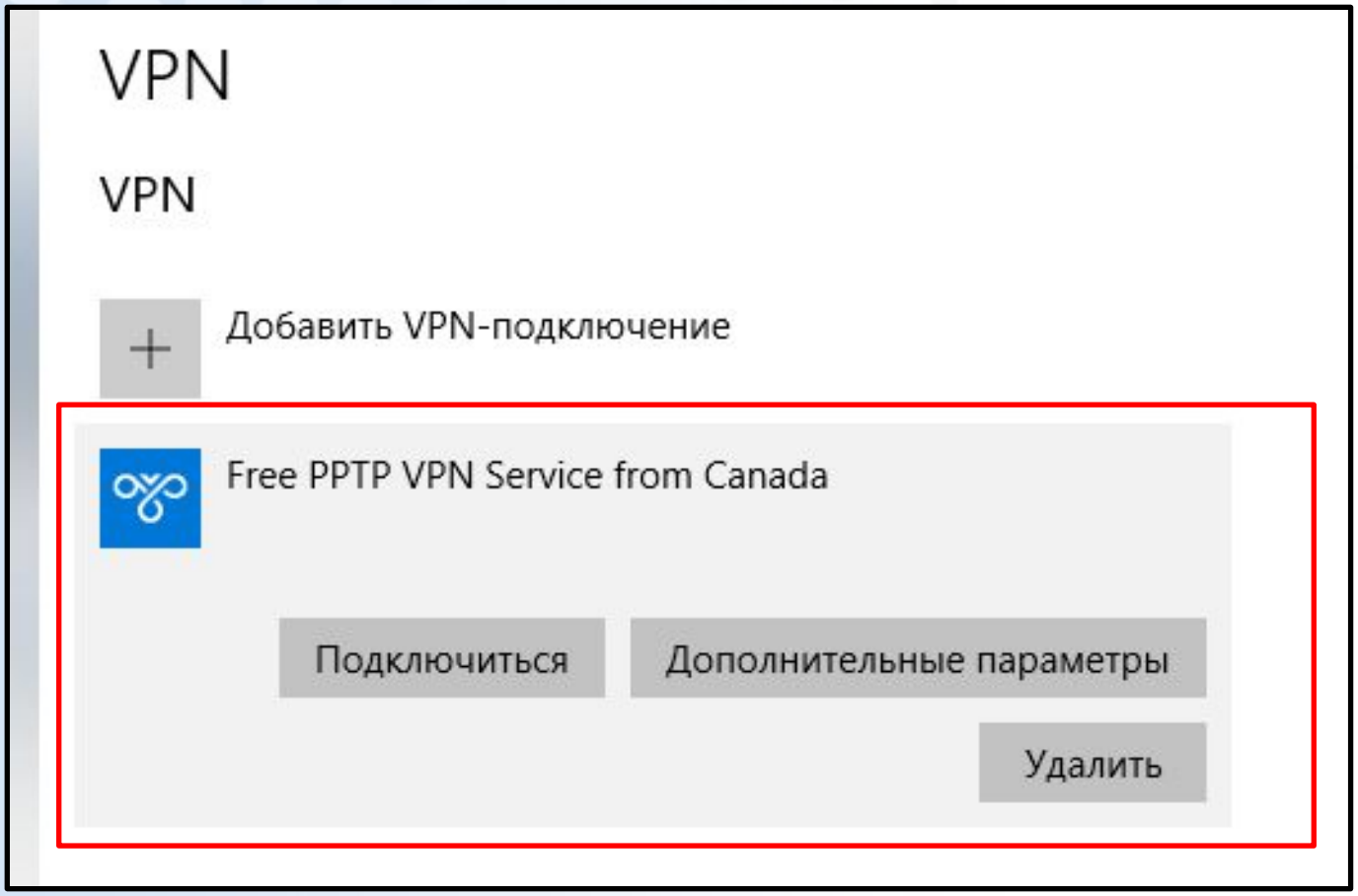
- Поставщик услуг VPN - Windows (встроенные)
- Имя подключения - название создаваемого подключения, например Free PPTP VPN Service from Canada
- Имя или адрес сервера - адрес VPN-сервера. Нажмите для получения списка серверов
- Тип VPN – Автоматически (будет выбирать от сложного к простому)

Указать идентификационные данные:

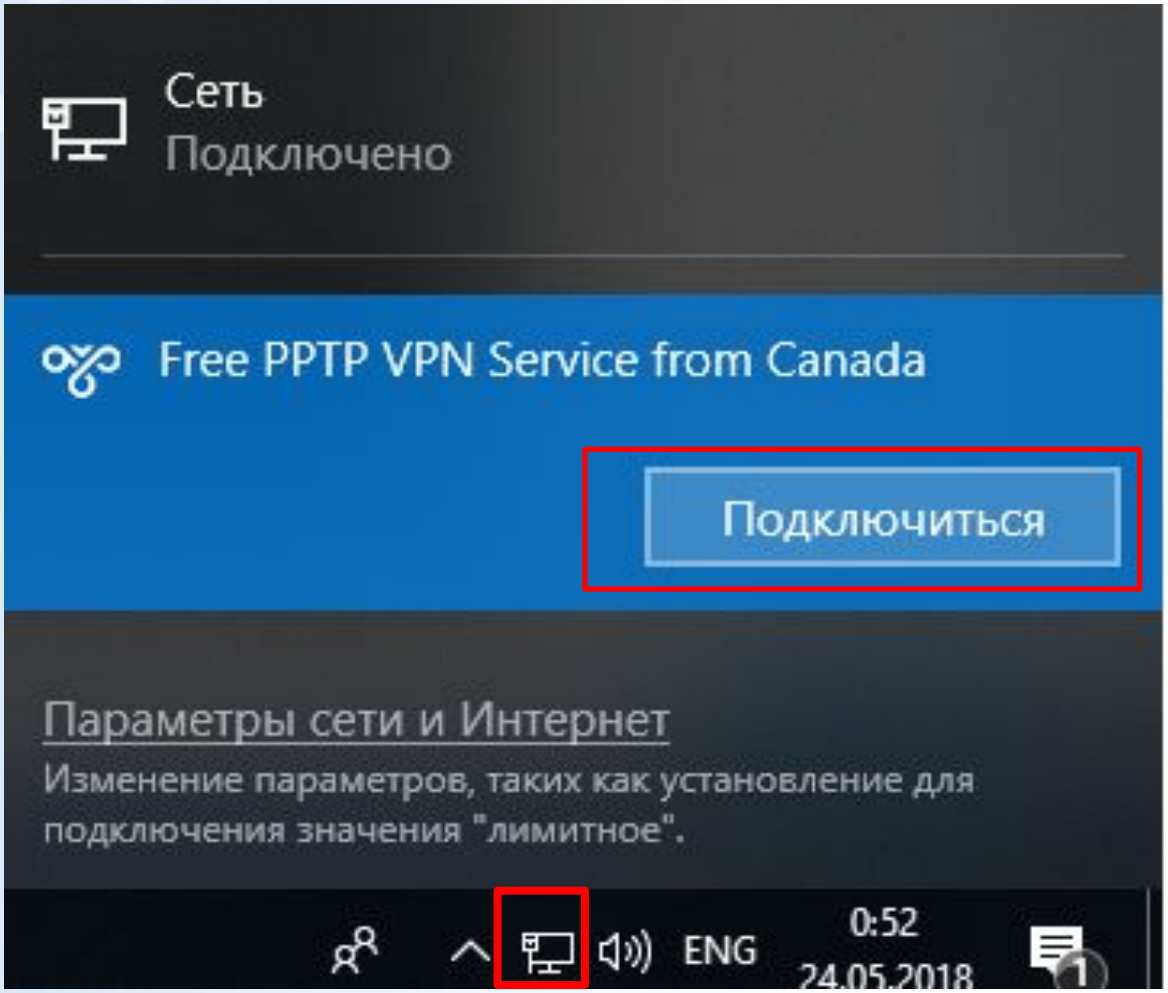
- Тип данных для входа - Имя пользователя и пароль
- Имя пользователя
- Пароль

Для завершения настройки нажать Сохранить.

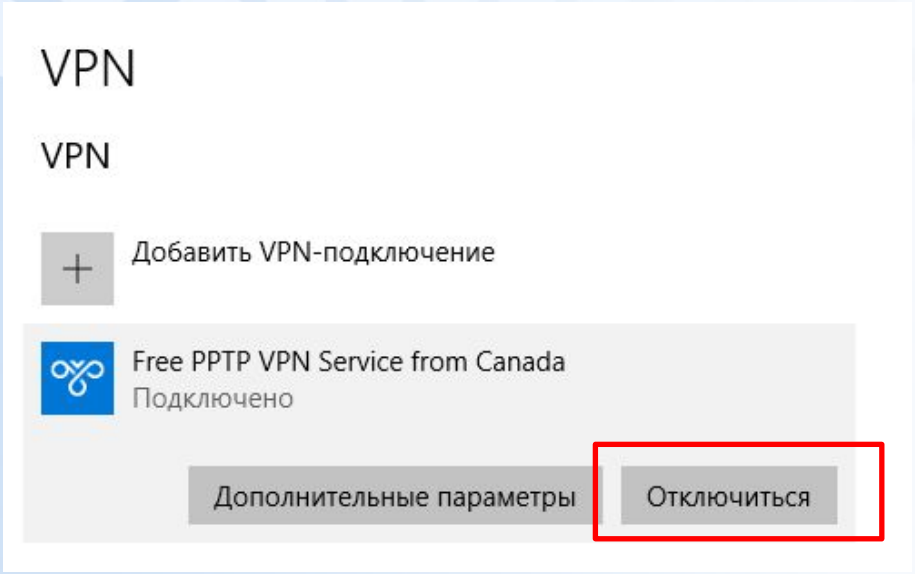
Для подключения:
1. выбрать только что созданное соединение, и нажать кнопку Подключиться.

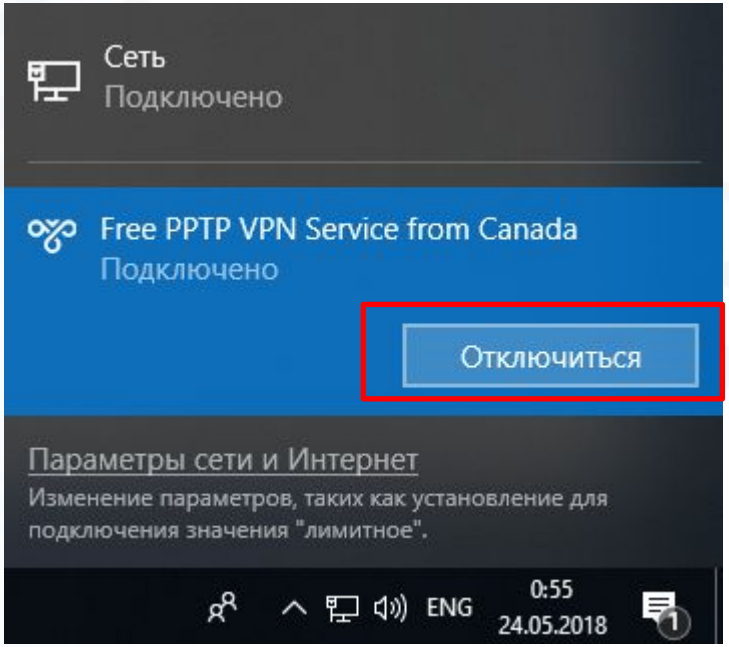


2. Кликнуть на иконке сетевого подключения в системном трее, в появившемся окне выбрать VPN подключение и кликнуть на Подключиться

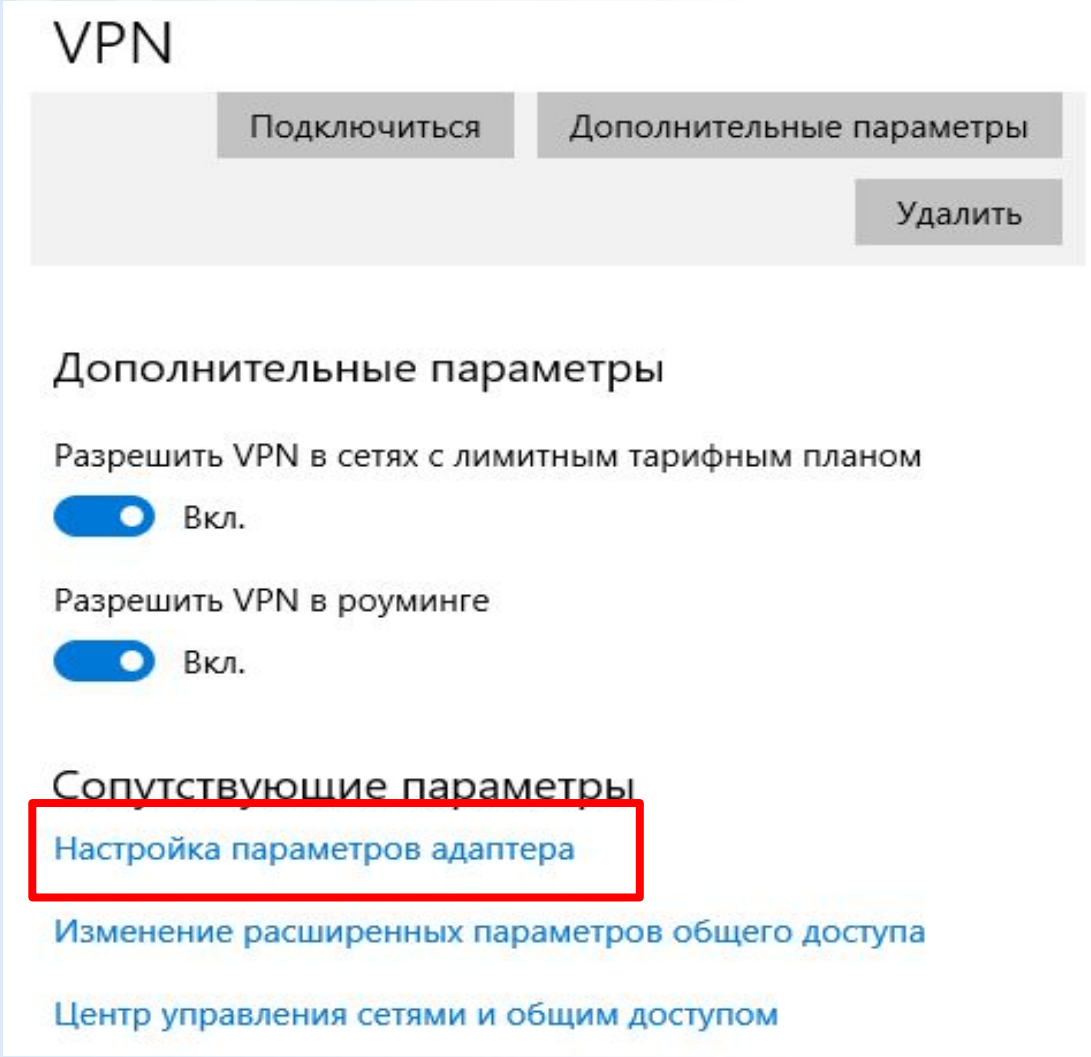


Соединение будет установлено через некоторое время.
Для отключения нажать Отключиться

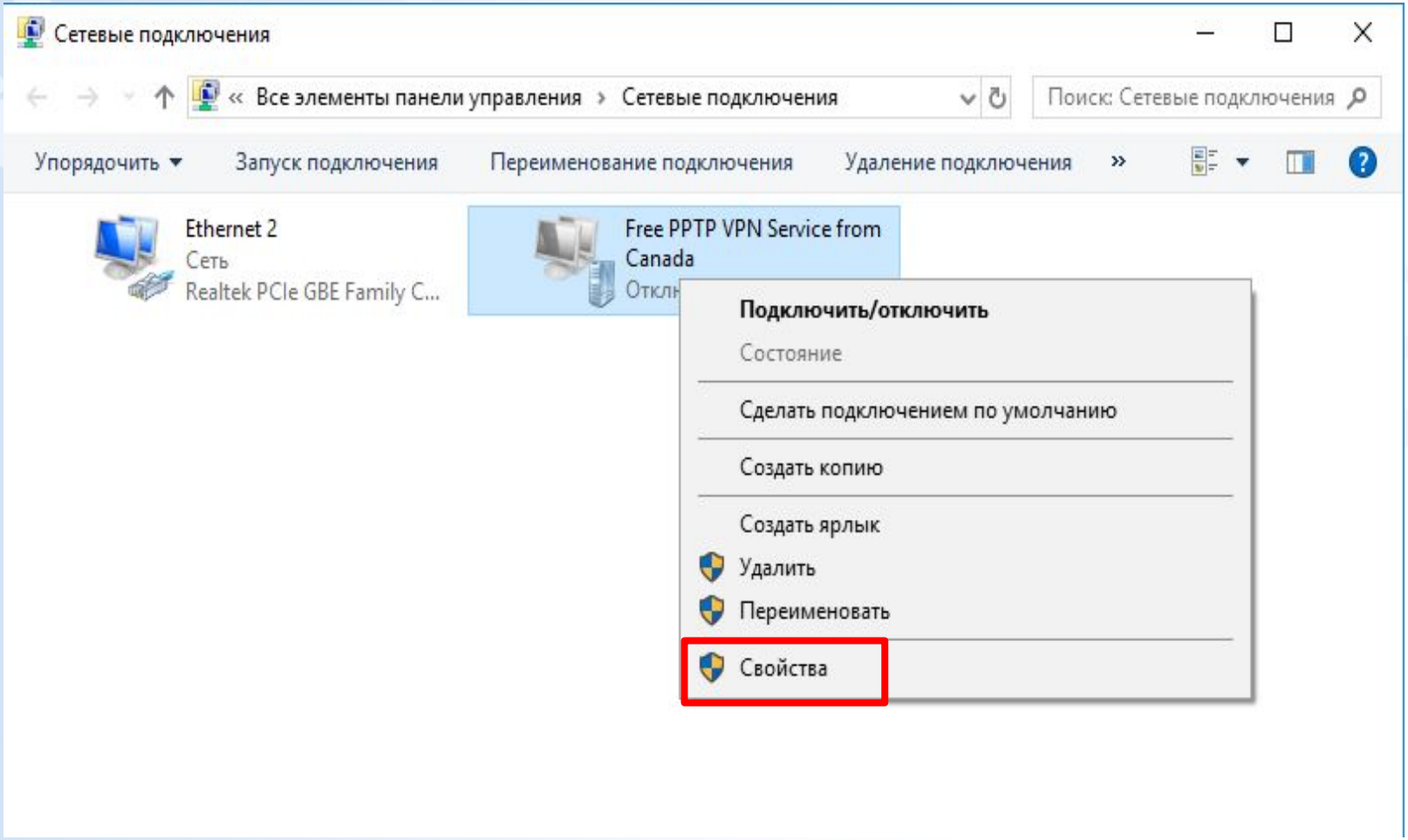




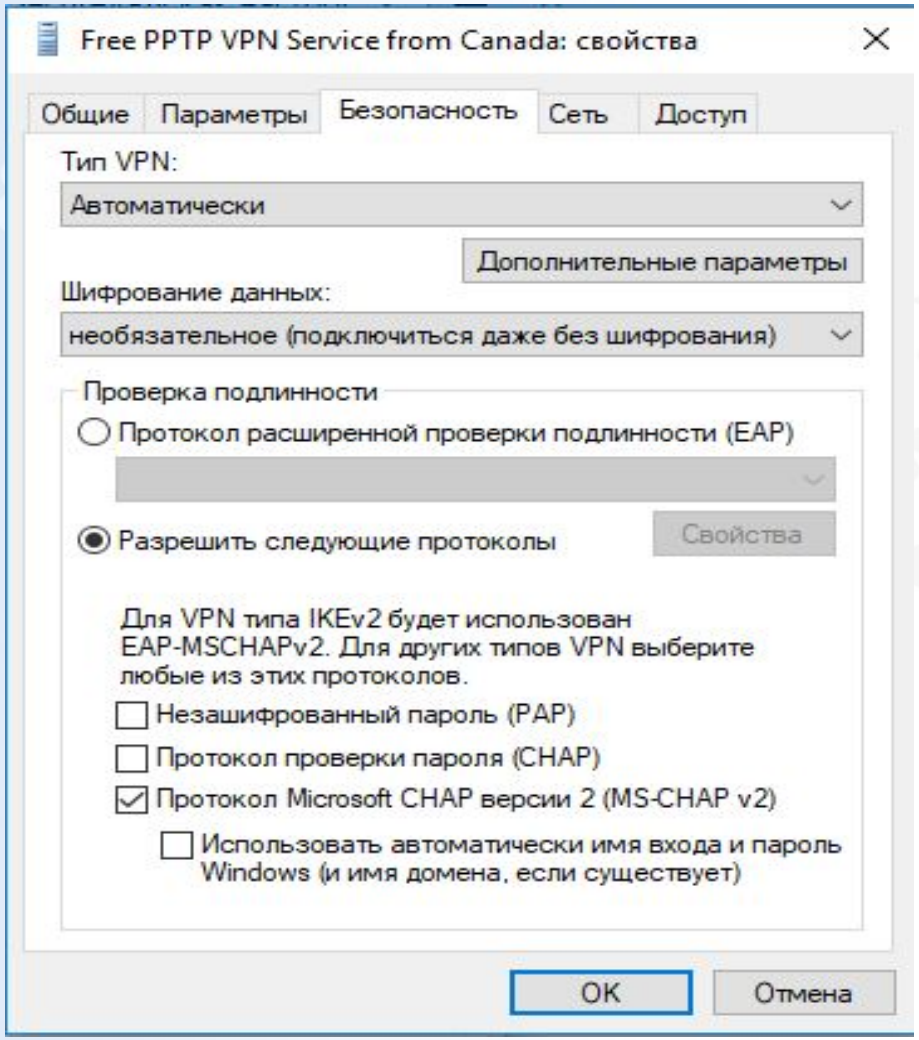
Для настройки дополнительных параметров подключения, повышающих уровень безопасности, выбрать Настройка параметров адаптера



В открывшемся окне Сетевые подключения кликнуть правой кнопкой на созданном подключении, и выбрать Свойства.



По умолчанию



На вкладке Безопасность выбрать шифрование - самое стойкое (отключиться, если нет шифрования).